METHOD FOR ELECTRONIC PAYMENT

[0001] This application is a continuation-in-part of U.S. application Ser. No. 11/061,616 filed on Feb. 22, 2005, European application number **04030898.3** filed on Dec. 28, 2004, U.S. application Ser. No. 10/964,654 filed on Oct. 15, 2004, and U.S. application Ser. No. 10/821,988, filed on Apr. 12, 2004, and claims the priority benefit thereof and which are incorporated by reference herein in their entirety.

FIELD OF THE INVENTION

[0002] This invention relates to payment methods in which a subscriber pushes credit or banking authorization to a vendor or merchant using the subscriber's mobile communications device. Actual credit card information may be supplied from on the mobile communications device or a remote database.

BACKGROUND OF THE INVENTION

[0003] Currently, consumers can purchase or shop while present at the merchant or vendor's location, or remotely, for instance by ordering over the telephone or through an electronic device over computer network like the internet. Payment for both local and remote purchases can be accomplished electronically by providing the merchant with an account identifier (credit card or debit card number, bank account number associated with a check, vendor's customer account, etc) through which payment can be authorized and funds can be transferred. The merchant generally receives the account identifier from the customer and bundles the identifier with the sale amount into a request for payment authorization. This request is generally forwarded electronically to an intermediary vendor to process the request for payment with the institution holding the customer's account, such as the credit card issuer, bank or other financial institution.

[0004] Such a payment system is subject to manipulation, theft and fraud due to the ease of access to the account information and difficultly in verifying the identifying of the person offering the account information as an authorized account user. For instance, if a credit card or credit card number is presented to the merchant, or input into an unsecured internet site, the merchant has access to the account information and the user's personal information, and such can be copied and later used by the unscrupulous employees for purchases. Scanning the card at the merchants location, or inputting a card into a secured internet site, can help alleviate theft of the consumers account information as the actual account information is not "visible" by the merchant's employees but is processed electronically. In a voice transaction, however, such as by ordering over the telephone, the account information is generally unprotected and subject to errors, particularly if a call center is handling the transaction.

[0005] The problems with theft of account information are well known, and various means have been implemented to combat theft and fraud. For instance, some account issuing institutions are now offering an "account identifier" that is valid for a single transaction. A more secure system is needed to handle payment transactions. In particular, as mobile cell phone technology becomes more prevalent, transactions initiated by cell phone are even more vulnerable due to unsecured nature of the cell path. The problem with cell technology will become event more aggravated due to the convergence of cell phones with internet enabled devices, such as the RIM Blackberry type services. With the expanding adoption of mobile cellular phones, a more secure system is needed to address payment systems for voice transactions. Today there is no method that allows a Purchaser to use a communications device to automatically transmit the Purchaser's pre-stored payment information (credit card number, bank account number, PIN, verification address, etc.) and other information necessary to complete a purchase. Additionally there is not a system that allows the financial institution to reduce its exposure to fraud by eliminating the verbal communication of credit or banking information, providing the additional security of having the Purchaser physically inputting a PIN number and the ability to grab the Purchaser's called ID or Internet address to further confirm the Purchaser's identity.

[0006] Transactions conducted over the Internet require the consumer to input the same information as required for a verbal order, which exposes the consumer to the possibility of the theft of the consumer's credit or debit card information and the consumer's personal data. Transactions where the card holder is not physically present are known as "card not present" or "MOTO" (mail order/telephone order) transactions.

[0007] Card Verification Value (CVV2) which is also known as CVC2 or Card Identification Number (CID) has been in use for over ten years. The system is basically a 3 digit or 4 digit numbers printed on the credit card separate from the actual credit card number and is not on the magnetic stripe. The merchant, whether via the Internet or telephone, asks for the number at the same time the card number is provided to the merchant. This number is then passed along to the verifying institution, which confirms that the card is in the presence of the cardholder. This method is subject to fraud, such as in the case of a criminal obtaining the credit card number may just as easily copy the CVV2 number. When cards are swiped and thus stolen electronically, the CVV2 number is copied at the time of the swiping and provided to whomever the card number is sold.

[0008] MasterCard's most recent security enhancement, in response to consumer demand for greater security and privacy in card not present transactions, implemented a system MasterCard named "MasterCard SecureCode". This system requires that the consumer, in an Internet transaction, to input a private code (that has been given to the consumer by the bank that issued the card), name address, etc., into a "pop-up" screen that appears on the Merchant's web page when the consumer has notified the web page that the consumer has completed the order. The consumer then inputs his/her private code and the authentication value is then passed along to the issuing bank in the merchant's normal authorization process. Using the MasterCard SecureCode system thus eliminates the possibility of "one click" purchasing, requires that the merchant install a SecureCode compliant "plug-in" application on the merchant's web site, and still provides the merchant with the consumer's credit card and other personal data. This method, while improving security over the previously existing system, is cumbersome and does not accomplish the objective of keeping the consumer's card number and personal information hidden from the merchant and improve ease of use by the cardholder. This method does not allow for notification to the